DOCUMENT RESUME

ED 095 588 CS 500 733

AUTHOR Stephens, Kent G.
TITLE A Fault Tree Approach to Analysis of Behavioral Systems: An Overview.
PUB DATE 74
NOTE 21p.

EDRS PRICE MF-$0.75 HC-$1.50 PLUS POSTAGE
DESCRIPTORS *Behavior Patterns; Communication (Thought Transfer); *Conceptual Schemes; *Decision Making; Higher Education; Models; *Systems Analysis; Systems Approach; *Systems Development
IDENTIFIERS *Fault Tree Analysis; FTA

ABSTRACT

Developed at Brigham Young University, Fault Tree Analysis (FTA) is a technique for enhancing the probability of success in any system by analyzing the most likely modes of failure that could occur. It provides a logical, step-by-step description of possible failure events within a system and their interaction--the combinations of potential occurrences which could result in a predetermined undesired event. The analysis for a fault tree begins with a precise statement about an undesired event of critical importance in a decision making process. This statement stands at the top of the tree, and the analysis proceeds downward. Contributing failure events are then interrelated by means of "logic gates" (e.g., AND and OR) to illustrate the cause and effect relationship which results in the undesired event. (A description of the FTA approach and its applications is included.) (RB)

A FAULT TREE APPROACH TO ANALYSIS OF BEHAVIORAL SYSTEMS

AN OVERVIEW

Kent G. Stephens, Ph. D.

Department of Educational Administration

Brigham Young University

A FAULT TREE APPROACH TO ANALYSIS OF BEHAVIORAL SYSTEMS

AN OVERVIEW

There are two basic approaches to analysis: (1) analysis in terms of success or accomplishment of system's purpose, or (2) analysis in terms of failure or non-accomplishment of a system's purpose. A systems approach may utilize either success or failure analysis.

Analysis in terms of success, however, is much more problematic than analysis in terms of failure. Not only is it difficult to achieve consensus as to those design characteristics and functions, the channels and interactions, which lead to system success, but experience has shown that in complex systems, it is much easier to describe and achieve consensus as to what constitutes failure. When a system is functioning smoothly, it is not at all easy to specify precisely what combinations of events contribute to this happy state. But when breakdowns occur, they are immediately apparent, although their causes and their "downstream" effects may be more obscure.

Fault Tree Analysis (FTA) is a technique for enhancing the probability of <u>success</u> in any system by analyzing the most likely modes of <u>failure</u> that could occur. It provides a logical, step by step description of possible failure events within a system and their interactions--that is, the combinations of potential occurrences which could result in a predetermined undesired event (U.E.). The fault tree was so named because the completed graphic portrayal of a functional system utilizes a branching process analagous to the outline of a coniferous tree.

It is not the intent of this paper to present a detailed explanation of the technique of performing a Fault Tree Analysis. Explanations of both qualitative and quantitative analysis, examples of educational and management information applications, and prototype trees may be found in Stephens (1972).

Description of Fault Tree Analysis

Following is a brief overview of the steps in Fault Tree Analysis. It should be noted that the fault tree approach can be used in a more simplified, abbreviated form, and still be very useful. In fact, decision makers have found that they could derive useful information from any of the steps followed in performing a fault tree analysis.

Qualitative Fault Tree Development

A fault tree consists of events, interrelated by logic gates, and resulting in complex pathways. The analysis begins with the precise statement of an undesired event (UE) of critical importance. It may be the failure of the entire system, expressed as a failure of the mission; or it may be a failure identified with some subsystem or component. In any event, it stands at the top of the tree, and the analysis proceeds downward. Inputs to the UE become contributing failure events in a cause and effect relationship.

Before discussing the nature of the events, however, it is necessary to clarify the concept of logic gates. The heart of the fault tree approach, and that which differentiates it from other forms of analysis, is the use of logic gates to show the relationships among events. There are two principal kinds of logic gates, the AND gate and the OR gate. All other gates used are derivatives of these two.

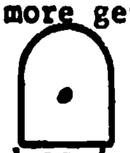
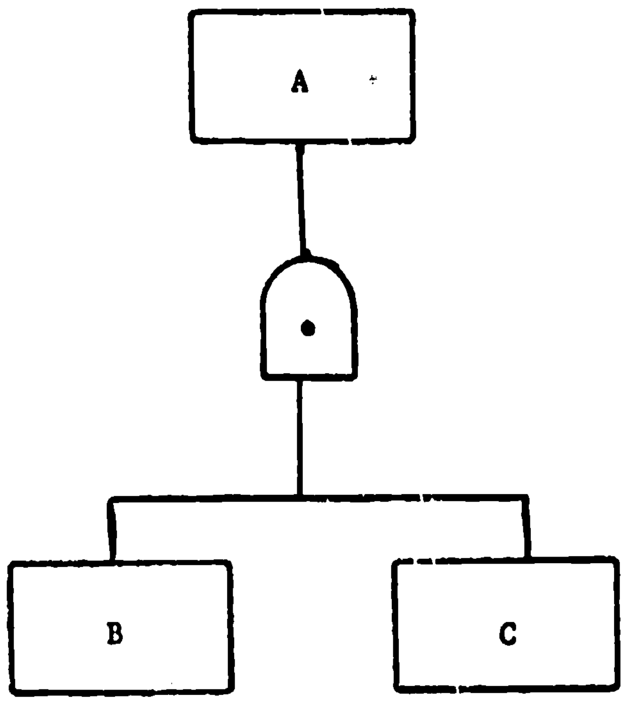
The AND logic gate is used when two or more events must coexist in order to produce the more general event. The AND gate is symbolized graphically by the symbol  . In the fault tree, events related by an AND gate would be depicted as in Figure 1.

Figure 1

THE AND GATE



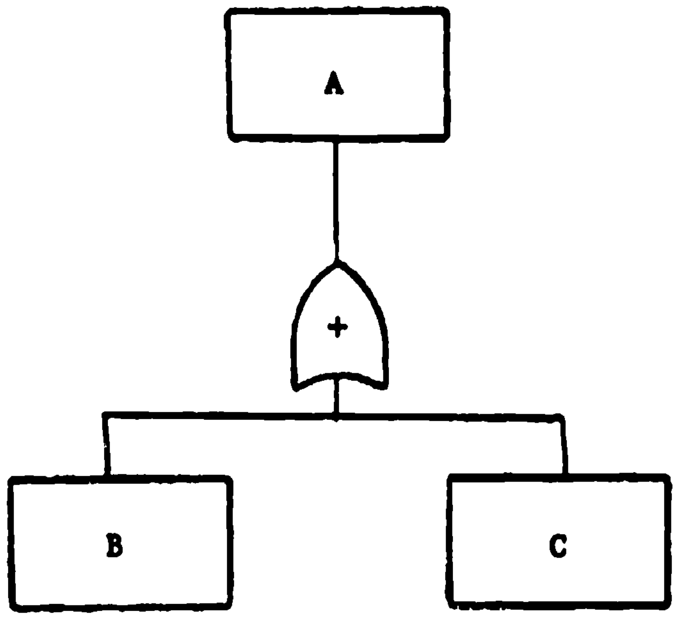
This would be read: Events B and C must coexist to produce Event A; or, the output can occur only if the inputs B and C coexist. The mathematical equivalent of this is $A = (B \wedge C)$.

In behavioral systems, this relationship most commonly exists when a subsystem or component and one or more backup systems or components exist or are possible within the design of the system. This situation occurs much less frequently in behavioral than in hardware systems, and the implications of this will be considered later in this paper in regard to the interpretation of the tree.

The OR logic gate is used when, of two or more possible inputs to an event, <u>any one</u> alone could produce the output. The graphic symbol for the OR gate is . In the fault tree, events related by an OR gate would be depicted as in Figure 2.

Figure 2

THE OR GATE



This is read: Either B <u>or</u> C alone will produce Event A. The mathematical equivalent of this is $A = (B \vee C)$.

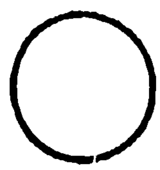
There are two general kinds of OR gates--the INCLUSIVE OR and the EXCLUSIVE OR. In the INCLUSIVE OR situation, <u>either</u> B <u>or</u> C <u>or</u> both could result in Event A. In the EXCLUSIVE OR situation, either A or B could produce C, but both A and B could not occur simultaneously.

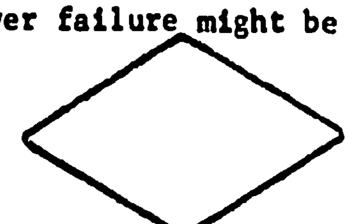
With either the AND or OR gates, more than two inputs may exist. Variations of these gates allow for the specification of complex relationships--there are inhibit gates, priority AND gates which specify the sequence of events, matrix gates, and others. The analysis thus provides precise description of conditions as well as modes of relationships, all of which can

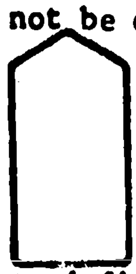
be expressed mathematically and quantified.

The other set of basic symbols used in fault tree analysis depicts the types of inputs or events. Input and output events can be classified according to their nature. The following are the most commonly used symbols for fault trees:

Rectangle:  Identifies an event that results from a combination of less general fault events through an associated logic gate. All events symbolized by rectangles have additional development in the fault tree.

Circle:  Identifies a basic failure event that requires no further development. This could occur when the definition of an event is sufficiently explicit to satisfy the purpose of the analysis. It also occurs when there is a "primary" failure of a component, analogous to a power failure in a telephone system. The decision as to whether the event is a basic one or not depends somewhat on the perspective of the analysis. For example, if the telephone system itself were being analyzed, then events leading to a power failure would be traced in much more detail. However, if a telephone is considered one system component within an organizational communication system, a power failure might be considered a basic event requiring no further analysis.

Rhombus:  Identifies an event which is not developed further due to (a) lack of information, (b) very remote likelihood of occurrence, or (c) because time, financial or other constraints preclude further analysis. (This symbol should not be confused with the diamond used as a decision point in flow charting.)

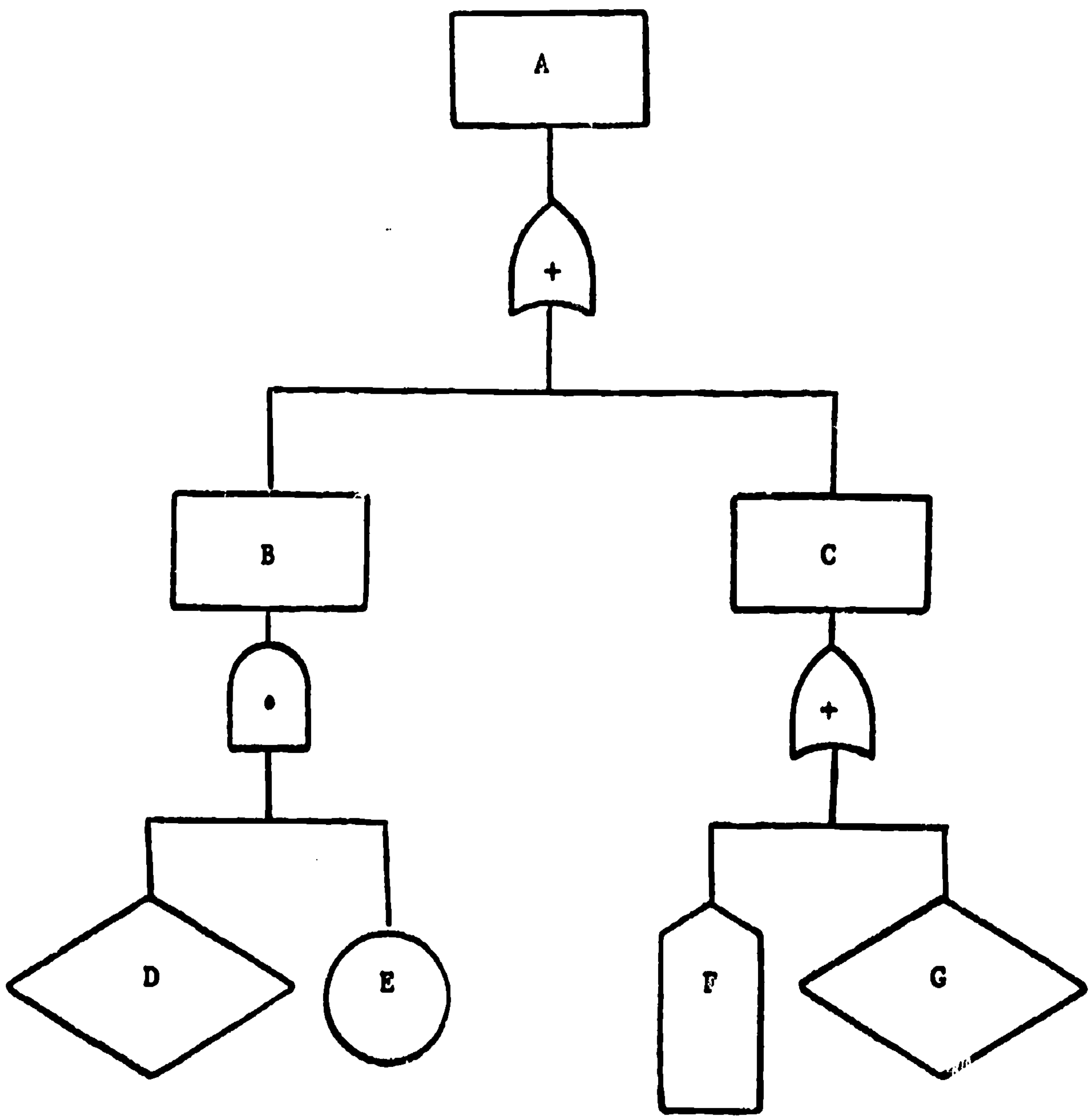
House:  Identifies an event that is normally expected to occur in the system as defined. When combined with other events, however,

it might contribute to a failure event.

Figure 3 shows a rudimentary fault tree, which is read as follows: "Event A can be produced _either_ by Event B _or_ Event C or both. Event B can be produced only by the coexistence of Events D _and_ E. Event C can be produced _either_ by Event F _or_ Event G or _both_." Event E is a primary or basic failure event, and Event F is an event that normally occurs in the system, but which can contribute to Event C. Events D and G require no further analysis.

Figure 3

ILLUSTRATION OF A FAULT TREE BRANCH



The "bottom of the tree" for any branch always will have events depicted by the circle, rhombus, or house. In this example, there are two branches and three levels of analysis.

For each given event, which in turn becomes a UE, failure events contributing to more general undesired events can be derived according to several models. One approach is to systematically ask questions regarding input, processing, output, and environmental factors; i.e., failures of a given component or subsystem may be attributable to failures of input from another part of the system, failures of processing within the component or subsystem itself, failures of output to another part of the system, or failures attributable to an abnormal environment. Inputs may be internal or external to the system, but in general, the more proximate the inputs in time or space to that failed component, the more powerful the analysis. If internal failure events are really due to events external to the system, they will usually show up at the points of interface between the system and its environment.

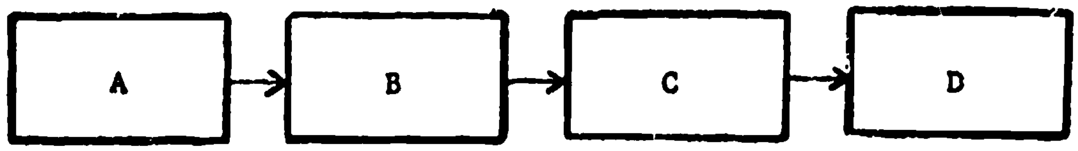
Figure 4 can be used to illustrate how failure analysis can be applied to a system which operates serially, Events A, B, and C being prerequisite conditions to Event D. In 4a the events are assumed to be operating successfully; i.e., for success of D, a single thread of events is necessary from A to B to C to D. In 4b the events are graphically analyzed for potential failure; that is, <u>failure</u> of D can be caused by failure of <u>either</u> A <u>or</u> B <u>or</u> C <u>or</u> any combination of them.

Figure 5 shows another possible system configuration, using both concurrent and prerequisite conditions for success. Diagram 5a assumes the system to be operating successfully. For success of D, the flow of events or information must go from A to B, then to C_1 or C_2 before D can occur. Diagram 5b shows the events as analyzed for potential failure. Failure of D can be caused only by

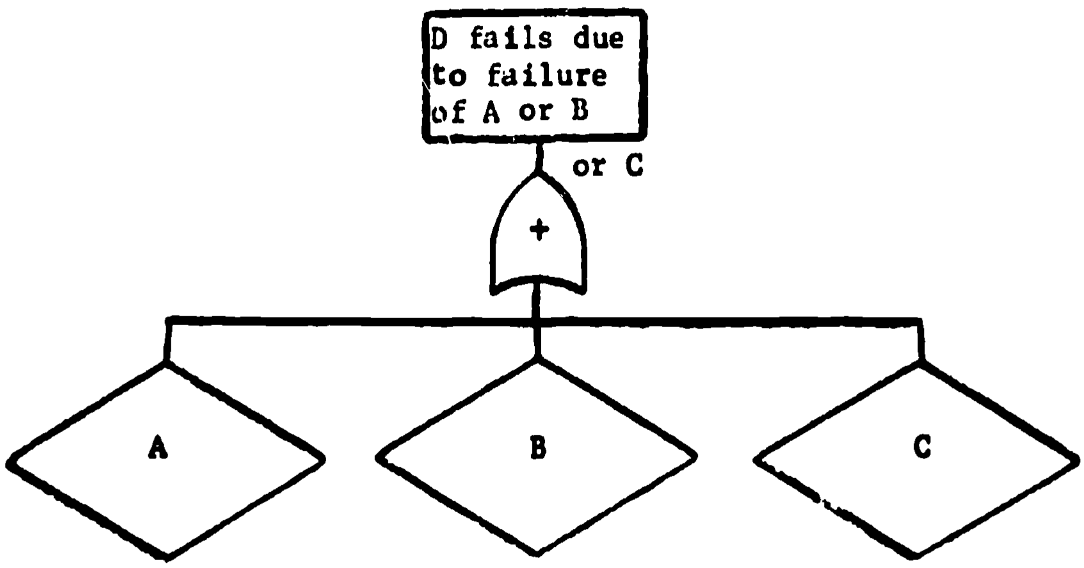
Figure 4

COMPARISON OF ANALYSIS IN SUCCESS SPACE WITH ANALYSIS IN FAILURE SPACE FOR PREREQUISITE EVENTS IN A SERIES

(a) system design



(b) failure analysis of above system design in terms of the failure of event D



(c) success analysis of system design in terms of the success of event D

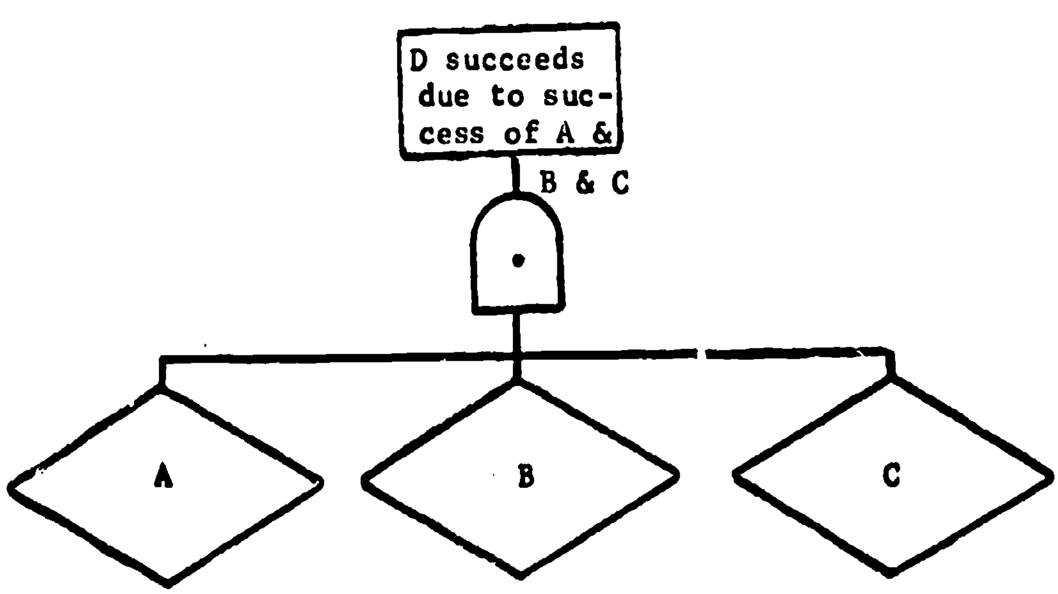
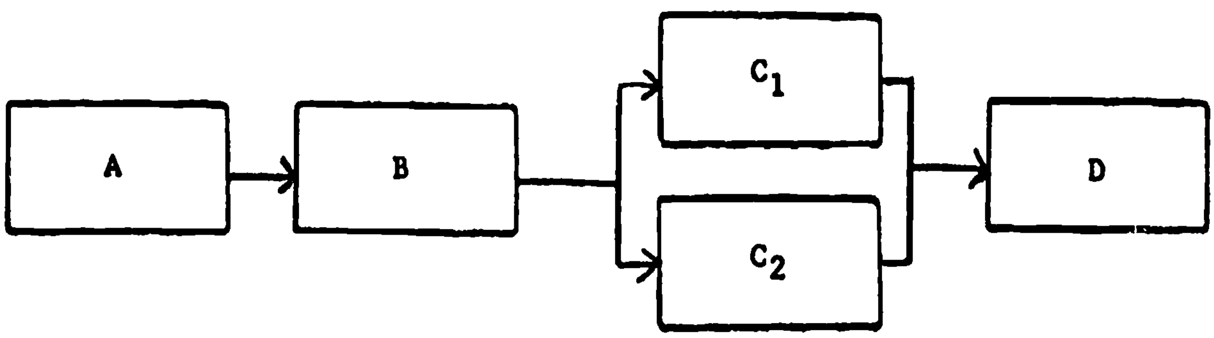


Figure 5

COMPARISON OF ANALYSIS IN SUCCESS SPACE WITH ANALYSIS IN FAILURE SPACE FOR CONCURRENT AND PREREQUISITE EVENTS

(a) system design



(b) failure analysis of above system design in terms of the failure of event D

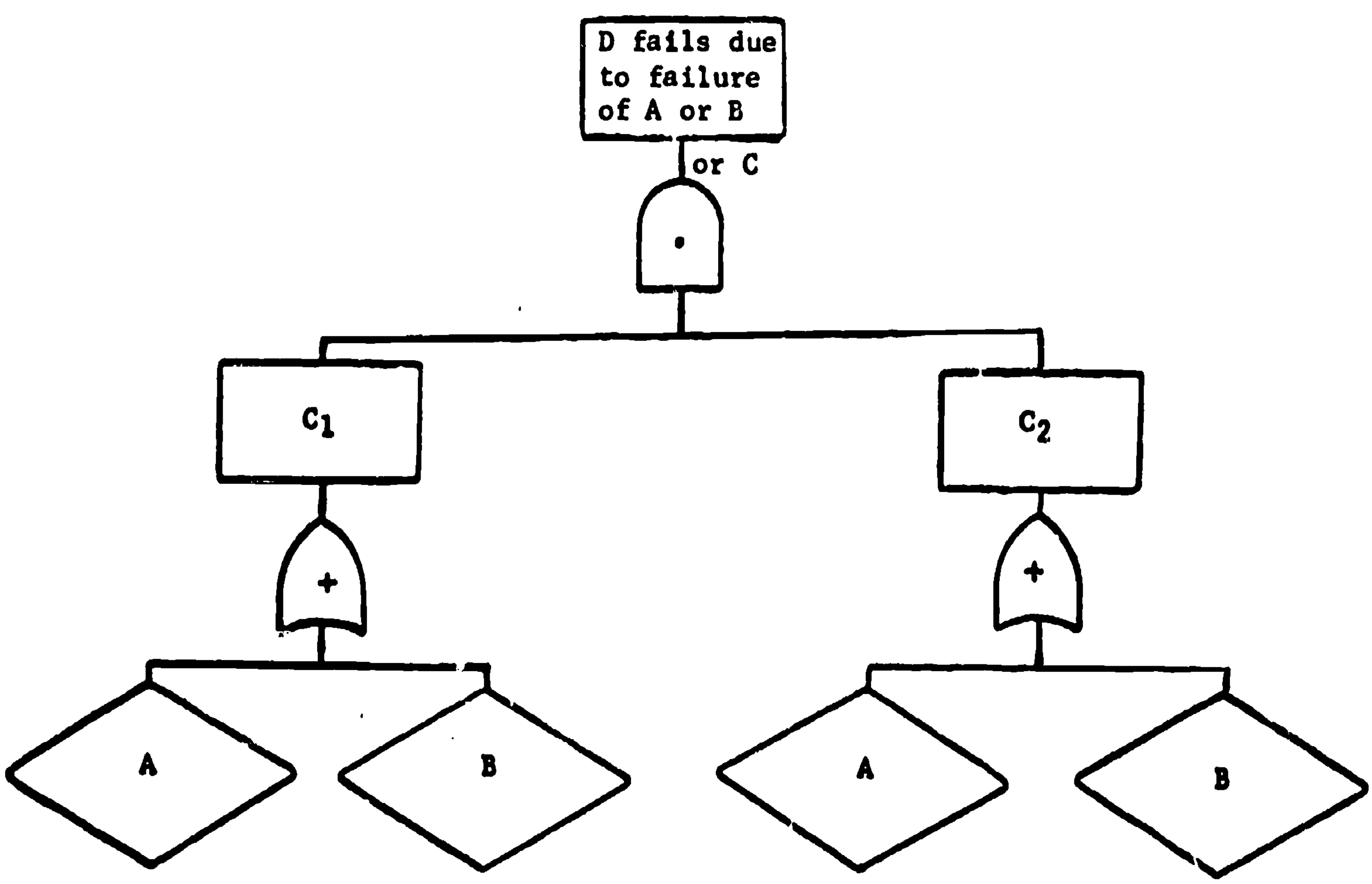
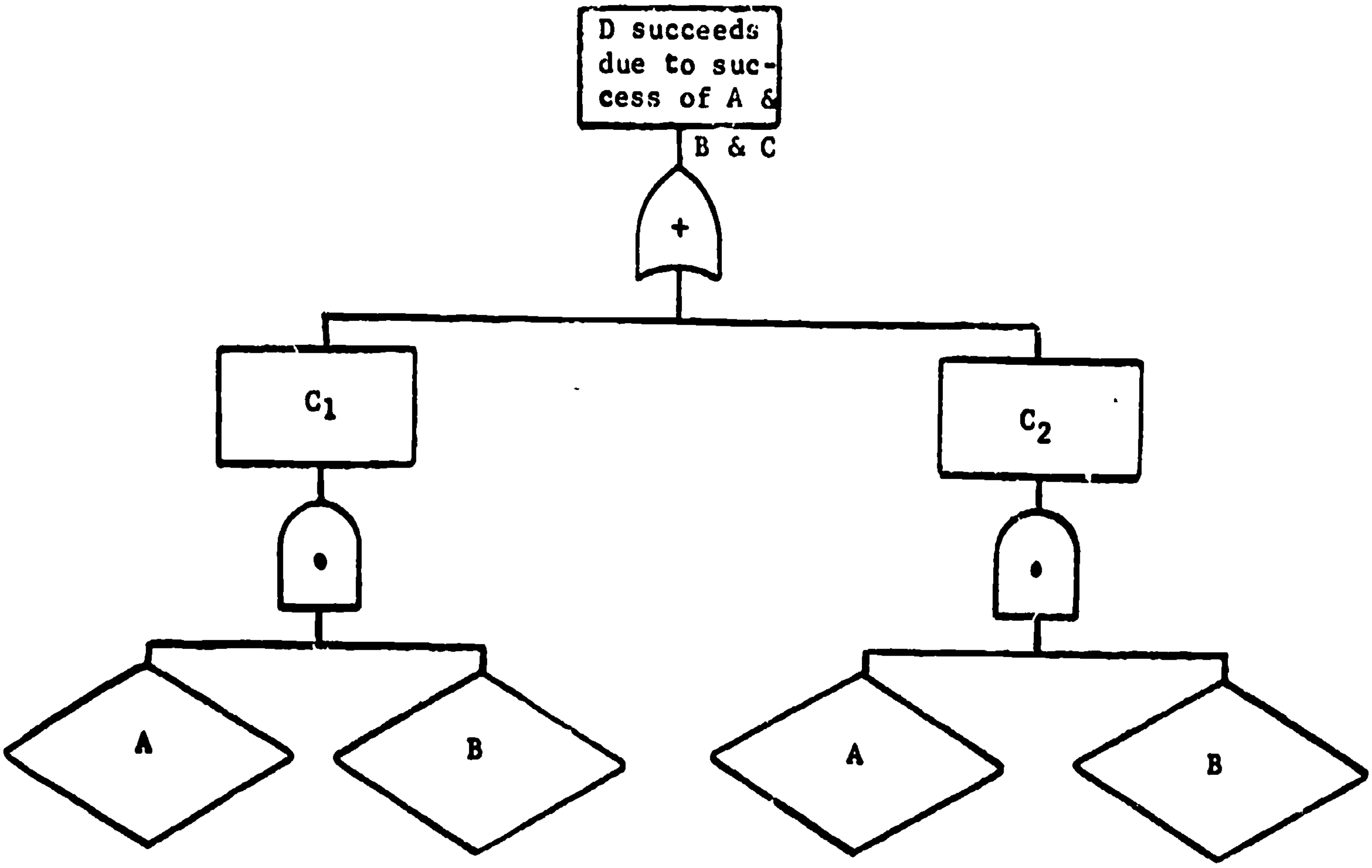


Figure 5
continued

(c) success analysis of system design in terms
of the success of event D



failure of C_1 and C_2 failing concurrently. C_1 can be caused by the failure of A <u>or</u> B or both; C_2 can also be caused by the failure of A or B or both.

In failure analysis, <u>any</u> event at the bottom of the tree which passes only through OR gates to more general failure events at the top of the tree becomes the same event, in essence, as the top UE. As an example in a behavioral system, or subsystem, such a configuration would occur when the flow of information can proceed only through specified channels, with no alternatives available in case of breakdowns, malfunctioning, or overloads. This is particularly serious when the system does not provide an alerting or monitoring mechanism, causing the problems to multiply before corrective

action can be taken. It should be apparent from Figures 4 and 5, however, that even a cursory inspection of system configuration will provide information as to the viability of the system, with consequent implications for changes in design and/or procedures.

Another point to note is that it appears from Figures 4 and 5 that analysis for failure is simply the logical reciprocal of analysis for success. To an extent this is true, in that experience has shown that reduction of the likelihood of an undesired event from occurring can be accomplished through changing or monitoring the sequences of events on the primary strategic paths determined on a fault tree.

Recent work with FTA of complex systems, however, has shown that failure analysis gives perspectives on a system which go beyond the simple logical inversion of success analysis to failure analysis and back again. In fact, the FTA methodology itself appears to have a heuristic value, both for those participating in the analysis and the managers and other decision makers to whom the results and recommendations are communicated. It generates questions about the system which do not occur under the usual conditions of success analysis. Additionally, the methodology, by facilitating consensus formation processes of groups, promotes team building activities which, in turn, lead to greater productivity.

Quantitative Fault Tree Development

Derive one or more strategic paths through quantitative Fault Tree Analysis (FTA)

Starting with the top UE, rank in order of relative contribution (or importance) of each of the failure events leading into it (i.e., each of the inputs), utilizing a consensus formation process such as the Delphi technique. (For a description of the technique applied to Fault Tree Analysis, see Stephens, 1972. More general sources are Helmer, 1966, Campbell and

Hutchin, 1968, and a comprehensive bibliography compiled by the Research Management Group of AERA.)

For all of the inputs to a single event, determine the percentage contribution made by each event to the more general failure event above it, utilizing a consensus process. Percentages should sum up to 100 for each event.

Repeat the above steps for the inputs to each failure event, working systematically down through the tree.

Decide on a rating scale suitable for use in evaluating the frequency (or likelihood) of occurrence of failure events in the fault tree. (E.g., a scale of low, medium, and high might use ratings of .1, .2, and .4 respectively, indicating that a "medium" rating is twice as likely to occur as a "low" rating, and that "high" is twice as likely as "medium." These are nominal values only.)

Determine the appropriate frequency rating for each event at the bottom or lowest level only for each branch of the tree. That rating for each input to an event is determined independently of the other inputs for that same event.

Calculate strategic path values for the tree utilizing the judgments of relative contribution, frequency of occurrence, and logic formulas through the logic gates. (For formulas, see Stephens, 1972.)

Identify strategic paths of interest by inspection.

Probability as a measure of the chance occurrence of events is usually defined mathematically as (a) the area under a curve which is representative of the pattern of occurrence of events, (b) the relative frequency of occurrence of events in a stochastic process, and (c) the ratio of the number of ways an event of interest can occur to the sum of the number of ways it can and cannot occur. Strategic path values do not give probabilities in

this sense, but they do represent a relative probability in the sense that they reflect measures of the occurrence of events in terms of how often those events might occur in the system (frequency) and how important they are if and when they do occur (relative contribution). The relationship of the probability formulas to logic diagrams is accomplished via Boolean algebra.

Although a computer program is available for deriving strategic paths (as well as for drawing the tree), the computations can be done by hand. On trees of more than 300-350 inputs, however, this process is too time consuming. Even without completing the quantification, however, much valuable information regarding the operation of the system can be gained by simple inspection of the tree.

It is not necessary for most of the team members engaged in qualitatively constructing the tree or quantifying it to know more than the rudiments of fault tree principles. The main requisite is a good working knowledge of the system under analysis. Team members should represent many different levels and functions within the organization, as the various "levels of visibility" afforded by different personnel will lead to perspectives differing in important respects. These perspectives are dealt with directly in the quantification process. Experience has shown that wide divergences of opinion can be reconciled without being ignored or subdued. Furthermore, the technique accommodates and utilizes both "hard" data and expert opinion.

An advantage of working with a Fault Tree is that the analyst can account for intermittent or fortuitous events while putting the information within a context in which reliable judgments can be made regarding the importance of such events and their contribution to failures of communication. Moreover, by focusing on the components of the system and its subsystems, rather than on individuals or types of messages, a general picture will emerge as to the extent to which the system fosters purposeful, goal-oriented communication,

or whether it sets up unnecessary barriers.

The degree to which a formal analysis is made will depend upon a number of factors--the amount of time available for analysis, the commitment of the organization to maximizing the communication system, the importance of the analysis to the organizational goals, and the perception of management of the general health of the system.

Recommending System Design Changes and/or Monitoring as Needed

The final step in FTA is to make recommendations based upon the strategic path analysis. These may include reallocating resources, installing backup systems, providing for monitoring of paths with high failure potential, redesigning subsystems, providing for improved communication at interfaces, or taking any other corrective action that seems advisable. Displaying the fault tree and discussing the strategic paths and their implications with personnel at various levels of the organization often will bring excellent suggestions for improvement and an increase in cooperative effort to work toward organizational goals.

History and Background of FTA

FTA is an operations research technique in which one form has been used with signal success as a major analytical tool of system safety engineering on aerospace projects. Rudimentary concepts of FTA originally were developed by Bell Telephone Laboratories as a technique for performing a safety evaluation of the Minutemen Launch Control System. Bell engineers discovered that the method used to describe the flow of "correct" logic in data processing equipment could also be used for analyzing the "false" logic resulting from component failures. (Haasl, 1965) The format was also well suited to the application of probability theory in order to define numerically the critical fault modes. Haasl points out that the Minuteman Safety Study was successfully completed

using the new technique, and provided convincing arguments for the incorporation of a number of equipment and procedure modifications.

Additional development of the analytical and mathematical techniques of Fault Tree Analysis in hardware systems occurred in the Boeing Company, and since it was first introduced in 1961, attempts have been made to apply the technique to many different systems inside and outside the company. Some of these have been a model of the man/machine interface in a manned space system, and analysis of such problems as highway safety and vandalism in the schools. For further descriptions of the history and development, see Ericson (1970) and Stephens (1972).

Driessen (1970) reports the application of FTA (which he calls Cause Tree Analysis) to industrial accidents, infant falls, and the like. He pleads for a wider application of the technique both to system safety analysis, and to psychology and the behavioral sciences.

Although a limited amount of analysis of human factors has been attempted, as in the Boeing man/machine interface of a manned space system, until 1967 few attempts had been made to apply the technique entirely to behavioral systems. This was partly because trained analysts were mainly engineers concerned with system safety, and partly because no adequate method of defining strategic paths (called critical paths in hardware fault trees) had been demonstrated. The nature of behavioral systems makes hard probability data difficult if not impossible to come by and such concepts as "time to repair" used in FTA hardware formulas have no exact human system counterpart.

Since 1967, however, the author has successfully applied FTA to a number of educational, managerial, and research problems, (Stephens, 1972, Witkin with Stephens, 1968), and have taught the technique to others during a two-year EPDA project (Witkin and Stephens, 1972).

An important breakthrough for FTA of non-hardware systems came with the development (Stephens, 1972) of a new quantification scheme for deriving strategic paths through the use of subjective probabilities. The viability of strategic path analysis for management decisions in educational systems was demonstrated through the author's analysis of the vocational educational system of the Seattle public schools, which resulted in a major curriculum change.

Since that time, both qualitative and quantitative FTA have been applied by the author, along with others who have taken FTA training, to other kinds of problems, including school district reorganization, a community college self study, and research project management. Additional applications include the formative evaluation of a university instructional television research project (Butler, 1972), and the analysis of communication breakdowns in the management of an ESEA Title III project for deaf children. FTA was also used as the principal management information system for Witkin's project in Auditory Perceptual Training, a three year research utilization project. FTA will also form the basis for cost/effectiveness analysis of the various modes of implementing and adapting the project's instructional materials to various media and classroom environments.

The FTA method used for generating inputs, tends to focus the thinking of the group on specifics and to organize all inputs within a systematic framework. Moreover, experience with very different kinds of fault trees (e.g., vocational education, research project management, community college assessment) has shown that the technique has other advantages in a multidisciplinary team effort.

1. It focuses expert knowledge and judgment from often widely disparate disciplines and functions on a common problem and furnishes a common language and perspective.

2. It can take into account both agreements and divergences on the inputs and their importance.

3. It allows for concentration on one area of interest at a time, but with the assurance that all other areas will be systematically dealt with.

4. By concentrating on the way the system operates, rather than on personalities, it introduces a non-threatening atmosphere and encourages a freer exchange of information among the members.

A serendipitous effect of FTA on participating members of an organization has been noticed. Without exception, those who have actively participated in working with the analyst to derive inputs for the qualitative and quantitative analysis have gained a new perspective of the system and have turned from somewhat passive members to active workers for system success. In one instance, in a large metropolitan school system, the FTA was so successful in engaging the support of the administration for a needed curriculum change, that the school board allocated over $200,000 additional to the area, at a time of stringent budget cutbacks. It might be added that the change was of a nature which would have been hotly fought in the past by the very people who became its proponents after working on the FTA.

A system approach to analysis must deal with the complexities and interdependencies which are an inherent part of any behavioral system. A characteristic of systems is that stress in any part of the system will eventually make itself felt in other parts, perhaps far removed from the stress point itself. It often happens, however, that a problem, such as a breakdown in communication, is perceived as having its source in one part of the system when, in fact, its "real" causes are elsewhere.

FTA is capable of dealing with such secondary effects of stress in the system, of spotting and analyzing redundant failure events which may have

significant cumulative impact, and of defining interactions among events which appear to be unrelated. The quantification process adds power to the qualitative analysis in accomplishing this.

To sum up. FTA has been found useful as the principal analytic method under the following conditions:

--Whenever undesired events or concerns and factors contributing to those concerns can be identified;

--Whenever differing areas of expertise must be marshalled;

--Whenever involvement of the members of an organization needs structure and systematizing;

--Whenever a defensible approach to resource allocation within a complex system is needed;

--Whenever consensus as to what constitutes success in the system is difficult to obtain;

--Whenever formative evaluation is necessary;

--Whenever the primary <u>and</u> secondary effects of future decisions must be analyzed.

Organizations both private and public often make plans which appear highly successful in solving social problems, only to have disastrous secondary effects appear, sometimes 25 years later. In commenting on the need for sophisticated tools to predict such secondary effects, Wilkinson (1972) wryly states,

> . . .on the shaky assumption that you can't act intelligently to solve a problem unless you know something about the system of which it is a part, it may eventually turn out that a systematic stab at social problems will at least enable those who are burdened with responsibility to consider such problems intelligently.

It is hoped that more decision makers will consider analysis for failure as well as analysis for success in system management.

REFERENCES

Archibald, Russel D. and Richard L. Villoria. Network-Based Management Systems. PERT/CPM. New York: John Wiley & Sons, Inc., 1968.

Burhans, David T., Jr. The Development and Field Testing of Two Internal Communication Measuring Instruments. Paper presented at the International Communication Association, Atlanta, Georgia, April 19-22, 1972.

Butler, Katharine G. Competency Programming in Special Education. First Progress Report. California State University at San Jose, Department of Special Education. Oct. 15, 1972.

Campbell, Robert M. and Hutchin, David. The Delphi Technique: Implementation in the Corporate Environment. Management Services, Nov.-Dec., 1968, pp. 37-42.

Campbell, Vincent N. and David G. Markle. Identifying and Formulating Educational Problems. A report to the Far West Laboratory for Educational Research. Palo Alto, California: American Institute for Research, Dec. 1967.

Cooper, Bernice. An Analysis of the Behaviors of Principals as Observed and Reported in Six Critical Incident Studies. Journal of Educational Research, 56:8, 1963, 410-414.

Driessen, Gerald J. Cause Tree Analysis: Measuring How Accidents Happen and the Probabilities of Their Causes. Paper presented at the 78th Annual Convention of the American Psychological Association, Miami Beach, Florida, Sep. 3-8, 1970.

Ericson, C. System Safety Analytical Technology--Fault Tree Analysis, 1970. The Boeing Company, Seattle, Washington. Report Number D2-113072-2.

Farace, Richard V. and Hamish M. Russell. Beyond Bureaucracy--Message Diffusion as a Communication Audit Tool. Paper presented at the International Communication Association, Atlanta, Georgia, April 19-22, 1972.

Flanagan, J. C. The Critical Incident Technique. Psychological Bulletin, 51:4, 1954, 327-258.

Franc, Max B. Assessment of Attitude and Opinion Change Effects of the Communication Audit. Paper presented at the International Communication Association, Atlanta, Georgia, April 19-22, 1972.

Greenbaum, Howard H. The Appraisal of Organizational Communication Systems. Paper presented at the International Communication Association, Atlanta, Georgia, April 19-22, 1972.

Haasl, David F. Advanced Concepts in Fault Tree Analysis. Paper presented at System Safety Symposium, University of Washington and the Boeing Company, Seattle, June, 1965.

Hawes, Leonard C. Information Overload and the Organization of 1984. Paper presented at the Western Speech Association Convention, Portland, Oregon, No. 23-25, 1970.

Helmer, Olaf. The Use of the Delphi Technique in Problems of Educational Innovations. P-3499. Santa Monica, California: RAND Corp., Dec. 1966.

Herzberg, Frederick. One More Time: How Do You Motivate Employees? Harvard Business Review, 46, Jan.-Feb. 1968, pp. 53-62.

Herzberg, Frederick. Work and the Nature of Man. New York: The World Publishing Company, 1971.

Inoue, Michael S. Systems Research for Research Systems. Paper presented at the First Annual Meeting, Far West Region, Society for General Systems Research, Sep. 14-16, 1972.

Katz, Daniel and Robert L. Kahn. Communication: The Flow of Information. In Larry L. Barker and Robert J. Kibler, Eds., Speech Communication Behavior, Prentice-Hall, Inc., 1971, pp. 81-87.

San Leandro Unified School District in cooperation with the Bureau of Elementary and Secondary Education, California State Department of Education. Foreign Language Dropouts. Problems and Solutions. 1970.

Stephens, Kent G. A Fault Tree Approach to Analysis of Educational Systems as Demonstrated in Vocational Education. Unpublished doctoral dissertation, University of Washington, 1972.

Wilkinson, John. Retrospective Futurology. The Center Magazine. 5:6, November/December 1972, pp. 59-62.

Witkin, Belle Ruth. Management Information Systems. Applications to Educational Administration. Alameda County PACE Center, 1971. ERIC ED 057-608.

Witkin, Belle Ruth and Kent G. Stephens. Inservice Training in Using Fault Tree Analysis as a Technique for Evaluation and Management of Vocational Education Programs. Interim report. EPDA Project 01-700-EF-001-71, Alameda County School Department, Hayward, California, Sep. 1971.